Remarks:

1.   <u>Rejections</u>

        Applicant acknowledges with appreciation that the Examiner has withdrawn the previous rejections. Nevertheless, claims 1-19 now stand rejected under 35 U.S.C. § 103(a), as allegedly rendered obvious by U.S. Patent No. 6,138,119 to Hall <u>et al</u>. ("Hall") in view of Published Patent Application No. US 2002/0023109 A1 to Lederer, Jr. <u>et al</u>. ("Lederer"). Applicant respectfully disagrees.

2.   <u>Obviousness</u>

        As noted above, claims 1-19 stand rejected as allegedly rendered obvious by Hall in view of Lederer. In order for the Office Action to establish a <u>prima facie</u> case of obviousness, at least three criteria must be met. First, the prior art reference or references must disclose or suggest all the claim limitations. Second, there must be some suggestion or motivation, either in the reference itself or the combined references or in the knowledge generally available to one of ordinary skill in the art, to combine or modify the cited references, in the manner proposed by the Office Action. Third, there must be a reasonable expectation of success. MPEP 2143. For the reasons set forth below, Applicant respectfully disagrees.

    a.   <u>Rights Management Versus Compliance Data</u>

        Hall describes a descriptive data structure 200 ("DDS") which is associated with a rights management data structure, <u>e.g.</u>, a newspaper 102 or a magazine 106. DDS 200 includes DDS definitions 202. The Office Action asserts that "Hall's 'rights management' reads on applicant's 'compliance data.'" Office Action Page 2, Lines 16-17. This is simply incorrect. "Rights management" consists of "[p]olicies, legislation, caveats and/or classifications [e.g., top secret, secret, etc.] which govern or restrict access to or use of records." Australian Government, National Archives of Australia, Recordkeeping Metadata Standards for Commonwealth Agencies, http://www.naa.gov.au/record/keeping/control/rkms/rights_management.html#2(2000) (copy enclosed). "Compliance data" does not govern or restrict access to data. Instead, according to Applicant,

> compliance data [is] data relating to regulations, guidance documents, and/or international and domestic standards. Compliance data may be generated by governments, regulators, agencies, national or international bodies, and like sources, and is utilized by the public for personal, commercial, or industrial applications. Compliance data informs, instructs, or guides users to act in accordance with a compliance authority's rules or expectations, <u>e.g.</u>, a product

manufacturer, such as a drug or medical device manufacturer, establishes procedures for shippers or couriers to eliminate or reduce mix-ups, damage, deterioration, contamination, or other adverse effects to a product during handling. However, because compliance data may be generated at a plurality of locations and by numerous sources, e.g., a plurality of remote web pages and sites on the Internet, a user is burdened by a large amount of navigation over the Internet or time consuming research through printed documents, or both. Further, a user may have to filter the compliance data of interest from large amounts of unwanted or unnecessary information. Moreover, compliance data may lack detailed organization or may be presented in data formats, which are cumbersome and not user friendly. Moreover, a user may not be familiar with a compliance data source's administration policy, e.g., a government agency's inspection policy, and may not have sufficiently developed database skills to locate the compliance data of interest. Thus, the current distribution and organization of compliance data makes it difficult for users to gather and utilize the compliance data in a beneficial or efficient manner.

Appl'n, Page 1, Line 20, through Page 2, Line 6. Thus, "[c]ompliance data, particularly standards, include information that serves as a rule for making judgements [sic] or as a basis for comparison, information authorized as the measure of quantity or quality, or information that serves as a standard or basis." Appl'n, Page 4, Lines 16-19. Consequently, unlike rights management, which is a set of rules governing or restricting access to content; compliance data is content.

According to Hall, access to data or content may be governed or restricted based on a the method by which the data is structured (e.g., formatted). For example, when the rights management data structure is newspaper 102, Hall's DDS definitions 202 define a generic format that a newspaper style publication could use. Specifically, a first DDS definition 202a does not specify a particular headline of newspaper 102, e.g., Yankees Win the Pennant, but instead defines a location of the headline within newspaper 102. Because DDS 200 is generic to a class or a family of style content publications, it can be reused. See, e.g., Hall, Column 10, Lines 58-68; and Column 11, Lines 1-3. In another example, when rights management data structure is magazine 106, because magazines typically do not include headlines or breaking news, DDS 200 may not define such formatting. Instead, DDS 200 for magazine 106 may define issue date, a magazine title, the name of the photographer, and associated artwork designation.

The essence of "rights management" using Hall's DDSs is that the content is known and categorized or formatted in advance of its search or use. Applicant understands that in rights management structures, security of the content is achieved because access to the content

may be authorized based on these divisions. To use Hall's metaphor, instead of trying to acquire information, the person seeking content obtains the prepackaged content of a rights management structure, similar to a "paint by numbers" painting kit. Hall, Column 3, Lines 20-33. Hall may describe some flexibility in the gaining access to information, but this flexibility is achieved by searching formatted containers; providing the format, so that others may produce compatible containers; or temporarily creating compatible containers, so that they may be accessed. Hall, Column 6, Lines 32-61.

Although the Office Action now seeks to combine Lederer's disclosure with that of Hall, the Office Action seems to rely on Lederer primarily to demonstrate that systems for ensuring compliance with regulations were known in the art. In particular, the Office Action asserts that "compliance data" comprising at least one requirement for complying with a standard regulation or law was known at the time that Applicant filed her application. Lederer, Paras. [0041] and [0042]. The Office Action, however, continues to rely on Hall for the disclosure of most of the steps of Applicant's claimed method and the elements of Applicant's claimed system. In view of the foregoing remarks, Applicant maintains that "rights management" does not read on "compliance data" and that to the extent that rights management governs or restricts access to data, data sorted to achieve access control does not disclose or suggest compliance data.

Because Hall's "rights management" does not read on Applicant's "compliance data," Applicant's compliance data may not be read into the Hall's system, as proposed by the Office Action. Consequently, Applicant maintains that the Office Action fails to demonstrate that Hall in view of Lederer discloses or suggests each and every element of the claimed invention. Therefore, Applicant respectfully requests that the Examiner reconsider the obviousness rejection in view of the foregoing remarks and withdraw the rejections to the pending claims.

b.   No Motivation or Suggestion to Combine

To the extent that Lederer describes "compliance data," the Office Action has demonstrated no suggestion or motivation for substituting a Lederer's compliance data for Hall's rights management data or descriptive data structures (DDS). As noted above, Hall describes the manipulation of DDS to provide an abstract representation of a rights management structure.

E.g., Hall, Abstract. A rights management structure is a method or system for providing secure digital containers to safely and securely store and transport digital content. Hall, Column 1, Lines 40-41. Referring to **Figs. 1A, 1B, 2A**, and **2B**, Hall describes how DDSs are used to divide identified elements of content (e.g., sections of a newspaper or magazine) within a data container. Not only may the content be divided in this fashion, but access to the content may be granted or denied based on these divisions. See, e.g., Hall, Column 4, Line 38, through Column 5, Line 4.

Hall determines a format and conforms the information for which access will be controlled to that format. The Office Action contends that it would have been obvious to a person skilled in the art to combine Lederer with Hall because "using the steps of 'said compliance data comprising at least one requirement for complying with at least one of standards, regulations and laws' would have given those skilled in the art the tools to set specific standards for the use in describing data that must abide by data rules. This gives users the advantage of maintaining the integrity level of transferred data in a network environment more efficiently." Office Action, Page 3, Lines 2-6. This may be a reason to combine Lederer with Hall, but this combination does not achieve the claimed invention and therefore, fails to support an obviousness rejection. Applicant's invention searches for compliance data from a plurality of compliance data sources and then edits the gathered data to include organizational data, i.e., searches and then modifies the data, and then imposes a format. Compliance data, by its very nature, must be available to all persons seeking to be in compliance. Applicant's claimed invention does not seek to restrict or govern access to any content. Instead, the claimed invention seeks to facilitate the gathering, editing (e.g., tailoring), storing, and delivering compliance data to the user seeking to comply. This is a fundamental difference between Hall and Applicant's claimed invention - a difference which is not bridged by Lederer.

Further, Hall describes the division of data into access limited containers. Such a division may be desirable when trying to govern or restrict access to the data. Nevertheless, such a division is contrary to the claims to and goals of Applicant's invention. Specifically, "it is another feature of the invention is [sic] that a central repository is provided to users to eliminate the need to search in multiple locations for data." Appl'n, Page 3, Lines 11-13; see also Appl'n, Page 1, Lines 27-31 (quoted above); Appl'n, Claim 1 ("gathering compliance data from at least one compliance data source . . . ").

DC01:394032.1

At least because Applicant's compliance data may not properly be equated to Hall's management rights, the Office Action has failed to demonstrate that a person of ordinary skill in the art would have been motivated to modify Hall to include Lederer's teaching with respect to compliance data to achieve Applicant's claimed invention. In addition, because of the fundamentally different goals of Hall's rights management system and Applicant's invention, the Office Action fails to demonstrate the required motivation or suggestion to combine Hall and Lederer. In the absence of such a motivation or suggestion to combine to achieve the claimed invention, the obviousness rejection of claims 1-19 is untenable. Therefore, Applicant respectfully requests that the Examiner reconsider the obviousness rejection in view of the foregoing remarks and withdraw the rejections to the pending claims.

CONCLUSION

Applicant respectfully submits that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that an interview with Applicant's representatives, either in person or by telephone, would expedite prosecution of this application, we would welcome such an opportunity. Applicant believes that no fees are due as a result of this response. Nevertheless, in the event of any variance between the fees determined by Applicant and those determined by the U.S. Patent and Trademark Office, please charge any such variance to the undersigned's Deposit Account No. 02-0375.

Respectfully submitted,

BAKER BOTTS LLP

Dated: July 28, 2004

By: _____

James B. Arpin
Registration No. 33,470
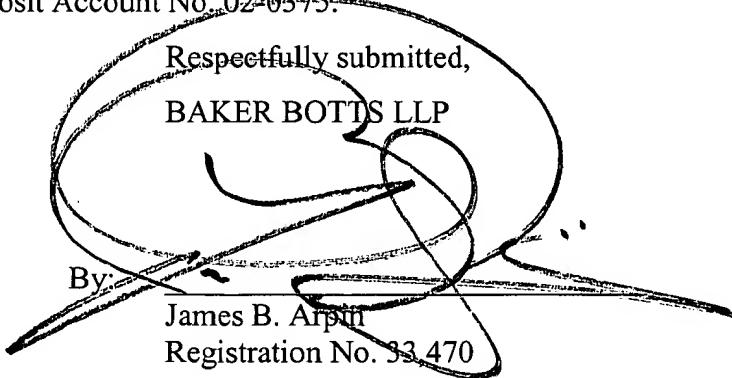
Baker Botts LLP
The Warner; Suite 1300
1299 Pennsylvania Avenue, N.W.
Washington, D.C. 20004-2400
(202) 639-7700 (telephone)
(202) 639-7890 (facsimile)

JBA/dh

Enclosure

DC01:394032.1

-6-

Home   About this Site   Site Map   Search   Links   Feedback

ABOUT US | THE COLLECTION | RECORDKEEPING | EDUCATION | EXHIBITIONS | PUBLICATIONS

Australian Government
National Archives of Australia

Recordkeeping Metadata Standard for Commonwealth Agencies

Element 2 – Rights Management

CONTENTS

Links from this page

2. Rights Management

Definition	Policies, legislation, caveats and/or classifications which govern or restrict access to or use of records.
Purpose	To facilitate the proper and appropriate management of sensitive or classified records. To alert users to restrictions on access and use of records, and to advise on when such restrictions may change or cease.
Rationale	Access to and use of records must be managed in accordance with relevant pieces of legislation and security policies to prevent damage to national security interests, and to protect the privacy of individuals and the business interests of corporate entities.
Obligation	Mandatory

Applicability	Sub-elements 2.1–2.4 are applicable at all levels of aggregation.
	Sub-elements 2.5 and 2.6 are generally applicable at Item and File levels only.
	Sub-element 2.7 is generally applicable at Item level only.
Use Conditions	The values contained in the sub-elements reflect the current status of access and usage rights for the records.
	The values shall be able to be changed by an authorised Agent ('authorised Agent' shall be agency-defined).
	When values for access and usage rights are changed, the old values shall be stored in element 15. MANAGEMENT HISTORY.
Repeatable?	No

Sub-elements	Name	Obligation	Schemes
	2.1 Security Classification	Mandatory	PSM, SECMANs
	2.2 Caveat	Optional	PSM, SECMANs, ACSIs, ASSROs and other domain-specific instructions
	2.3 Codeword	Optional	ASSROs, other agency- or domain-specific instructions
	2.4 Releasability Indicator	Optional	SECMANs, PSM, agency- or domain-specific indicators
	2.5 Access Status	Optional	Freedom of Information (FOI) Act, agency-specific
	2.6 Usage Condition	Optional	Privacy Act, Copyright Act, agency-specific instructions, policies or procedures which govern how an agency's records can be used
	2.7 Encryption Details	Optional	GPKI: public key (DEA)

Comments	-

2.1 Security Classification

Definition	A means of classifying records based on their security requirements.
	There are two categories of classification – 'National Security' and 'Sensitive' (non-National Security). The differences between National Security and Sensitive material are defined in Part III of the *Protective Security Manual*. The classifications for National Security material are Restricted, Confidential, Secret and Top Secret. The classifications for Sensitive material are In-Confidence, Protected and Highly Protected.

Purpose	To minimise the chances of records being acquired by people or organisations not authorised to receive them. Agencies dealing with classified material are required to ensure that it is given the appropriate levels of protection to prevent its unauthorised disclosure and subsequent damage to government or national security interests. Penalties apply if classified material is not adequately protected.
Obligation	Mandatory
Conditions	It shall not be possible to use element 7. RELATION to relate a single item of a particular security classification with a file of a lower classification level – eg it shall not be possible to use sub-element 7.2 Relation Type, Assigned Value 'Contains/Contained In' to associate a secret item with a confidential or unclassified file. The value of this sub-element may change over time, so it shall be linked to element 15. MANAGEMENT HISTORY , sub-element 15.2 Event Type, Assigned Value 'Classification Up/Downgraded'. When 'Classification Up/Downgraded' is selected as the action to be taken on the record, the old value of the Classification sub-element shall be replaced by the new value. Details of the change, including the old classification, shall be placed in MANAGEMENT HISTORY. Also refer to sub-element 15.2 Event Type.

Assigned Values	Value Name	Definition
	Unclassified	Definitions are as laid down in
	Restricted	
	Confidential	the SECMANs for Defence agencies
	Secret	
	Top Secret	and the *Protective Security Manual* (PSM)
	In-Confidence	
	Protected	for non-Defence agencies.
	Highly Protected	

Default Value	Unclassified. Shall also have the capability to be changed and set by an agency, according to the security domain within which it operates – ie it shall be possible to set the default to the 'system high' value of a particular agency system.
Repeatable?	No
Assigned By?	The default value shall be system-generated. Changes to the default value shall be manually selected from a pick list by an agent, such as the Record Creator.
Schemes	PSM, SECMANs, ACSIs.
Comments	-

2.2 Caveat

Definition	A warning that the record requires special handling, and that only people cleared and entitled to see that record may have access to it.
Purpose	To help prevent unauthorised handling of, or access to, records with special sensitivities. Agencies are required to ensure that records with special caveats are properly handled and adequately protected against unauthorised access. Penalties may apply if caveated material is not adequately protected.
Obligation	Optional
Conditions	Other caveats may be added as Assigned Values by agencies working within particular security domains or compartments. The value of this sub-element may change over time, so it shall be linked to element 15. MANAGEMENT HISTORY , sub-element 15.2 Event Type, Assigned Value 'Caveat Changed'. When 'Caveat Changed' is selected as the action to be taken on the record, the old value of the Caveat sub-element shall be replaced by the new value. Details of the change, including the old caveat, shall be written to the MANAGEMENT HISTORY. Also refer to sub-element 15.2 Event Type.
Assigned Values	**Value Name** / **Definition** Cabinet-in-Confidence — Definitions for caveats are laid down in Commercial-in-Confidence — SECMANs for Defence agencies, Medical-in-Confidence — PSM for non-Defence agencies, Staff-in-Confidence — in the DSD ACSIs, and in other domain- Personal — specific instructions such as ASSROs.
Default Value	A default value shall be able to be set by an agency in order to meet its own requirements.
Repeatable?	Yes
Assigned By?	The default value shall be system-generated. Changes or additions to the default value shall be manually selected from a pick list by an agent, such as the Record Creator.
Schemes	PSM, SECMANs, ACSIs, ASSROs, other agency- or domain-specific instructions.
Comments	-

2.3 Codeword

Definition	A form of caveat which is used to refer to classified information or

	activity, without revealing the nature of that information or activity to unauthorised personnel.
Purpose	To prevent discovery of the nature of the information or activity covered by particular security compartments. To provide a shorthand means of referring to classified material of a specific nature, thereby protecting the nature and purpose of that material from discovery by people without the relevant briefings.
Obligation	Optional
Conditions	The value of this sub-element may change over time, so it shall be linked to element 15. MANAGEMENT HISTORY , sub-element 15.2 Event Type, Assigned Value 'Codeword Changed'. When 'Codeword Changed' is selected as the action to be taken on the record, the old value of the Codeword sub-element shall be replaced by the new value. Details of the change, including the old codeword, shall be written to the MANAGEMENT HISTORY. Also refer to sub-element 15.2 Event Type.
Assigned Values	Most codewords are highly domain-specific and need to be specified by the agencies concerned.
Default Value	A default value shall be able to be set by an agency in order to meet its own requirements.
Repeatable?	Yes
Assigned By?	The default value shall be system-generated. Changes or additions to the default value shall be manually selected from a pick list by an agent, such as the Record Creator.
Schemes	ASSROs, other agency- or domain-specific instructions.
Comments	-

2.4 Releasability Indicator

Definition	A self-evident abbreviation applied to certain records to indicate their releasability status, such as whether they may be released to another country.
Purpose	To restrict the dissemination of the records to certain nationalities. To provide a further level of protection against the compromise of national security interests.
Obligation	Optional
Conditions	The value of this sub-element may change over time, so it shall be linked to element 15. MANAGEMENT HISTORY , sub-element 15.2 Event Type, Assigned Value 'Releasability Indicator Changed'.

	When 'Releasability Indicator Changed' is selected as the action to be taken on the record, the old value of the Releasability Indicator sub-element shall be replaced by the new value. Details of the change, including the old caveat, shall be written to the MANAGEMENT HISTORY. Also refer to sub-element 15.2 Event Type.
Assigned Values	**Value Name** **Definition** AUSTEO Australian Eyes Only AUSCANUKUS Releasable to Australia, Canada, United Kingdom and United States
Default Value	A default value shall be able to be set by an agency in order to meet its own requirements.
Repeatable?	Yes
Assigned By?	The default value shall be system-generated. Changes or additions to the default value shall be manually selected from a pick list by an agent, such as the Record Creator.
Schemes	SECMANs, PSM, agency- or domain-specific indicators.
Comments	The above values are listed as examples only. There are many other possible values for Releasability Indicators (RIs), and these may be added as Assigned Values by agencies working within particular domains or compartments.

2.5 Access Status

Definition	Information about whether a record in the closed period (ie a record which is less than 30 years old) may be released or published, or whether it is to be wholly or partially withheld from public access.
Purpose	To facilitate or restrict public access to government records in the closed period.
Obligation	Optional
Conditions	The value of this sub-element may change over time, so it shall be linked to element 15. MANAGEMENT HISTORY , sub-element 15.2 Event Type, Assigned Value 'Access Status Changed'. When 'Access Status Changed' is selected as the action to be taken on the record, the old value of the Access Status sub-element shall be replaced by the new value. Details of the change, including the old access status, shall be written to the MANAGEMENT HISTORY. Also refer to sub-element 15.2 Event Type.
Assigned Values	**Value Name** **Definition** Not for Release The record is not to be released or published. May be Published The record may be published.

	May be Released under FOI	The record contains no information which might preclude it from being released to an individual or party under an FOI request.
	Limited Release	Due to particular sensitivities of a national security, privacy, business or other nature: the record may be released to a limited (agency-defined) audience only; or limited parts or sections only of a record may be released.
	Published	The record has been made publicly available (through formal publishing or some other means).
Default Value	Depending on its business requirements, an agency may set the default to be either 'Not for Release' or 'May be Published'.	
Repeatable?	No	
Assigned By?	A default value shall be system-generated. Any changes to the default value will be selected from a pick list by the agent – generally an Authority or a Records Manager.	
Schemes	*Freedom of Information Act 1982* (FOI Act), agency-specific.	
Comments	Agencies may be required to provide access to records under the provisions of the FOI Act. This sub-element applies only to records in the closed period, over which agencies have full control (subject to the provisions of the FOI Act, and restrictions imposed on the basis of privacy and/or national security interests). This sub-element should not be confused with the authority of the National Archives, under the *Archives Act 1983*, to examine and determine the access status of records in the open period (ie records over 30 years of age). The National Archives remains the authority in this area, and will continue to record access status information for records in the open period in its CRS system.	

2.6 Usage Condition

Definition	An indication that some kind of limitation or restriction has been placed on how a record may be used by staff within an agency or by the general public.
Purpose	To protect a record against any form of unauthorised use (including unauthorised disclosure), or any use which may place the owner or creator of a record (either a corporate entity or an individual) at a disadvantage. To help an agency ensure that the records for which it is responsible are not used in ways that contravene copyright or privacy restrictions, or that will cause damage to specific business or domain interests.
Obligation	Optional

Conditions	Some Usage Conditions may be system-enforceable and will require specific usage types to be included under element 16. USE HISTORY, sub-element 16.2 Use Type, to track authorised usage and unauthorised attempts at usage over time.
Assigned Values	-
Default Value	Copyright © Commonwealth of Australia YYYY may be the default for a published Item. It shall be possible for an agency to set its own default value for the Usage Condition.
Repeatable?	Yes
Assigned By?	The default value shall be system-generated. Any changes or additions to the default value shall be selected by an agent from a pick list of assigned values defined by the agency.
Schemes	Privacy Act, Copyright Act, agency-specific instructions, policies or procedures which govern how an agency's records can be used.
Comments	There are many possible values for Usage Conditions. Examples include copyright statements, statements which detail to whom use of the record is restricted, and statements which list penalties for unauthorised disclosure. Other Usage Conditions may be added as Assigned Values by agencies to meet their own requirements for restricting the use of records.

2.7 Encryption Details

Definition	Information, or pointers to information, about how a record has been encrypted.
Purpose	To enable decryption (and hence, access) if the record is stored in the recordkeeping system in an encrypted state. To enable re-encryption if the record is stored in the recordkeeping system in a decrypted state, but needs to be moved to another system or location. If encryption is used, details need to be recorded about the public and private keys, and the Certification Authority which has authorised, and which vouches for, the identity of the key holders. These details are required in order to restrict or enable access to the encrypted record.
Obligation	Optional
Conditions	Shall be used if the record is covered by a digital signature – ie if sub-element 1.11 Digital Signature has been used.
Assigned Values	-
Default Value	The agency's own public key and Certification Authority.

Repeatable?	No
Assigned By?	System shall be able to automatically sense and record encryption details.
Schemes	GPKI: public key encryption (DEA)
Comments	This sub-element could be used either to record the encryption details themselves (if the recordkeeping system is considered sufficiently secure), or to record the location of the encryption details which are stored outside the recordkeeping system. It is recommended that information regarding private keys never be held within the recordkeeping system.

Rights Management Examples

Security Classification	Unclassified
Access Status	Published
Usage Condition	© Commonwealth of Australia 1999

Security Classification	In-Confidence
Access Status	May be released under FOI

Security Classification	Protected
Caveat	Cabinet-in-Confidence
Access Status	Limited Release

Security Classification	Secret
Caveat	Commercial-in-Confidence
Codeword	[Domain-specific]
Releasability Indicator	AUSTEO
Access Status	Not for Release
Usage Condition	Use by British Aerospace defence contractors and JP66270 project staff only

Encryption Details	Held in Vault 2

LINKS FROM THIS PAGE

Top of page

Next Element (3. Title)

Previous Element (1. Agent)

Back to the Recordkeeping Metadata Standards contents page

Back to the Control and Retrieval summary page